Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

Information Security Appendix – Socio Technical and Organisational Measures

1. Scope

This Appendix outlines the information security requirements between Customer and Socio and describes the technical and organizational security measures that shall be implemented by Socio to secure Personal Data prior to any Processing under the Agreement.

2. General Security Practices

Socio has implemented and shall maintain appropriate technical and organizational measures designed to protect Personal Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this Appendix for its personnel, equipment, and facilities at Socio's locations involved in Socio's performance of its obligations under the Agreement.

3. General Compliance

3.1. Compliance. Socio shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Personal Data given the risk posed by the nature of the data Processed by Socio. Socio shall implement and operate information security in accordance with Socio's own policies, which shall be no less strict than the information security requirements set forth in this Information Security Appendix.

3.2. Protection of records. Socio shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

3.3. Review of information security**.** Socio's approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

3.4. Compliance with security policies and standards**.** Socio's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

3.5. Technical compliance review**.** Socio shall regularly review information systems for compliance with Socio's information security policies and standards.

3.6. Information Risk Management ("IRM")**.** Socio shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Threat and vulnerability assessments must be periodically reviewed and prompt remediation actions taken where material weaknesses are found.

3.7. Processing of Special Categories of Personal Data**.** To the extent that Socio Processes Special Categories of Personal Data and the security measures referred to in this Information Security Appendix are deemed to provide insufficient protection, Customer may request that Socio implements additional security measures.

4. Technical and Organizational Measures for Security

4.1. Organization of Information Security

a. Security Ownership. Socio shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

b. Security Roles and Responsibilities. Socio shall define and allocate information security responsibilities in accordance with Socio's approved policies for information security. Such policies

Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

(or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

c. Project Management. Socio shall address information security in project management to identify and appropriately address information security risks.

d. Risk Management. Socio shall have a risk management framework and conduct periodic (i.e., at least annual) risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Personal Data.

4.2. Human Resources Security

a. General. Socio shall ensure that its personnel are subject to confidentiality obligations and shall provide adequate training about relevant privacy and security policies and procedures. Socio shall further inform its personnel of possible consequences of breaching Socio's security policies and procedures, which must include disciplinary action, including possible termination of employment for Socio's employees and termination of contract or assignment for Representatives and temporary personnel.

b. Training. Socio personnel with access to Personal Data shall receive appropriate, annual periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Personal Data and training regarding how to effectively respond to security incidents. Training shall be provided before Socio personnel are granted access to Personal Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

c. Background Checks. Socio shall conduct criminal and other relevant background checks for its personnel in compliance with mandatory applicable law and Socio's policies.

4.3. Personnel Access Controls

a. Access.

i. Limited Use. Socio will not use any system access information or log-in credentials to gain unauthorized access to Personal Data or Customer's systems, or to exceed the scope of any authorized access.

ii. Authorization. Socio shall restrict access to Customer's Personal Data and systems at all times solely to those Representatives whose access is necessary to perform the Services or provide the Products.

iii. Suspension or Termination of Access Rights. At Customer's reasonable request, Socio shall promptly and without undue delay suspend or terminate the access rights to Personal Data and systems for any Socio's personnel or its Representatives reasonably suspected of breaching any of the provisions of this Information Security Appendix; and Socio shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

iv. Information Classification. Socio shall classify, categorize, and/or tag Personal Data to help identify it and to allow for access and use to be appropriately restricted.

b. Access Policy. Socio shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Socio shall maintain a record of security privileges of its personnel that have access to Personal Data, infrastructure, and infrastructure services. Socio shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.

c. Access Authorization.

i. Socio shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Customer's data. Socio shall require revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

ii. Socio shall maintain and update a record of personnel authorized to access systems that contain Personal Data and Socio shall review users' access rights at regular intervals.
iii. For systems that process Personal Data, Socio shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.
iv. Socio shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

d. Network Design. For systems that process Personal Data, Socio shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Personal Data.
e. Least Privilege. Socio shall limit access to Personal Data to those personnel who need access for the purpose of providing the Services and Products and, to the extent technical support is needed, its personnel performing such technical support.
f. Authentication
i. Socio shall use industry standard practices to identify and authenticate users who attempt to access information systems.
ii. Where authentication mechanisms are based on passwords, Socio shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).
iii. Where authentication mechanisms are based upon passphrases, Socio shall require the passphrase to contain a minimum of 12 non-repeating characters.
iv. Socio shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.
v. Socio shall monitor repeated failed attempts to gain access to the information system.
vi. Socio shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.
vii. Socio shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.
viii. Socio shall implement a multi-factor authentication solution to authenticate personnel accessing its information systems.

4.4. Physical and Environmental Security
a. Physical Access to Facilities
i. Socio shall ensure limited access to facilities where systems that Process Personal Data are located to authorized individuals.
ii. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.
iii. Facilities shall be monitored and access-controlled at all times (24x7).
iv. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Personal Data. Facility operators must register personnel and require them to carry appropriate identification badges.
b. Physical Access to Equipment. Socio equipment used to process or store Personal Data shall be protected using industry standard processes to limit access to authorized individuals.
c. Protection from Disruptions. Socio shall ensure appropriate measures designed to protect against loss of data due to power supply failure or line interference are implemented.
d. Clear Desk. Socio shall have policies requiring a "clean desk/clear screen" designed to prevent inadvertent disclosure of Personal Data.

Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

4.5. Operations Security

a. Operational Policy. Socio shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data and to its systems and networks. Socio shall communicate its policies and requirements to all persons involved in the Processing of Personal Data. Socio shall implement the appropriate management structure and control designed to ensure compliance with such policies and with mandatory applicable law concerning the protection and Processing of Personal Data.

b. Security and Processing Controls.

   i. Areas. Socio shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks and services that store or Process Personal Data.

   ii. Standards and Procedures**.** Such standards and procedures shall include security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

c. Logging and Monitoring. Socio shall maintain logs of administrator and operator activity and data recovery events related to Personal Data.

4.6. Communications Security and Data Transfer

a. Applications. Socio shall, at a minimum, use the following controls to secure its application infrastructure that access or Process Personal Data:

   i. Network traffic shall pass through firewalls, which are monitored at all times. Socio must implement intrusion detection systems and/or intrusion prevention systems.

   ii. Utilities and systems used for administration must utilize industry standard cryptographic controls when Processing Personal Data.

   iii. Anti-spoofing filters and controls must be enabled on routers.

   iv. Administrative consoles, application, and system authentication passwords are required to meet minimum complexity guidelines (at least 8 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days for user-level accounts and ever 90 days for administrator-level accounts; or utilize other strong log-in credentials (e.g., passphrases, biometrics, etc).

   v. Initial user passwords or passphrases are required to be changed at first log-on. Socio shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

   vi. Firewalls must be deployed to protect the perimeter of Socio's environments.

b. Virtual Private Networks ("VPN"). When remote connectivity to the Customer's or Socio's network is required for Processing of Personal Data:

   i. Connections must be encrypted using industry standard cryptography.

   ii. Connections shall only be established using VPN servers.

   iii. The use of multi-factor authentication is required.

c. Data Transfer. Socio shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this Information Security Appendix. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

4.7. System Acquisition, Development, and Maintenance

a. Security Requirements. Socio shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. Development Requirements. Socio shall have policies for secure development, system engineering, and support. Socio shall conduct appropriate tests for system security as part of acceptance testing processes. Socio shall supervise and monitor the activity of outsourced system development.

Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

4.8. Penetration Testing and Vulnerability Scanning & Audit Reports

a. Testing**.** Socio will perform periodic vulnerability scans and penetration tests on its internet perimeter systems. These scans and tests will be conducted by highly qualified professionals, including among other entities, Socio's security team, using industry standard tools and methodologies.

b. Audits and Certifications**.** Socio shall cooperate with reasonable requests by Customer for legally required security audit (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Socio shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 18–SOC2 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Socio maintains such certifications in its normal course of business. Customer shall treat the contents of reports related to Socio's security and certifications as confidential information.

c. Remedial Action**.** If any penetration test or vulnerability scan referred to in Section a, above reveals any deficiencies, weaknesses, or areas of non-compliance, Socio shall promptly take such steps as may be required, in Socio's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable considering Socio's prioritization of such, based upon their criticality (e.g. nature, severity, likelihood).

d. Status of Remedial Action**.** Upon request, Socio shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

4.9. Contractor Relationships

a. Policies. Socio shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this Information Security Appendix.

b. Monitoring. Socio shall monitor and audit service delivery by its Representatives and review its Representatives' security practices against the security requirements set forth in Socio's agreements with such Representatives. Socio shall manage changes in Representative services that may have an impact on security.

4.10. Management of Data Breaches and Improvements

a. Responsibilities and Procedures. Socio shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.

b. Reporting Data Breaches**.** Socio shall implement procedures for Data Breaches to be reported as appropriate. All employees and Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.

c. Reporting Information Security Weaknesses**.** Socio, employees, and Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

d. Assessment of and Decision on Information Security Events**.** Socio shall have an incident classification scale in place in order to decide whether a security event should be classified as a Data Breach. The classification scale should be based on the impact and extent of an incident.

e. Response Process**.** Socio shall maintain a record of Data Breaches with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

4.11. Information Security Aspects of Business Continuity Management

a. Planning. Socio shall maintain emergency and contingency plans for the facilities where Socio information systems that process Personal Data are located. Socio shall verify the established and implemented information security continuity controls at regular intervals.

Socio Labs, LLC.
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

b. Data Recovery. Where and as applicable, Socio shall design redundant storage and procedures for recovering data in its possession or control in a manner sufficient to reconstruct Personal Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.